VDE-2025-074: Phoenix Contact: Security Advisory for CHARX SEC-3xxx charging controllers

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Oct 14 12:00:00 CEST 2025	Engine: 2.5.37
Current release date: Tue Oct 14 12:00:00 CEST 2025	Build Date: Wed Oct 15 10:21:01 CEST 2025
Current version: 1.1.0	Status: FINAL
CVSSv3.1 Base Score: 8.8	Severity: High
Original language:	Language: en-GB
Also referred to: VDE-2025-074, PCSA-2025-00015	

Summary

A vulnerability in the firmware of CHARX SEC-3xxx charging controllers has been discovered.

General Recommendation

For general information and recommendations on security measures to protect network-enabled devices, refer to the application note: Application Note Security.

Impact

The vulnerability can lead to a total loss of confidentiality, integrity and availability of the devices.

Mitigation

Affected charging controllers are designed and developed for the use in closed industrial networks. Phoenix Contact therefore strongly recommends using the devices exclusively in closed networks and protected by a suitable firewall.

Remediation

Phoenix Contact strongly recommends to upgrade to firmware version 1.7.4 which fixes vulnerability CVE-2025-41699

Product Description

CHARX SEC EVSE charging controller

Product groups

Affected products.

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

- FW <1.7.4 installed on CHARX SEC-3150
- FW <1.7.4 installed on CHARX SEC-3100
- FW <1.7.4 installed on CHARX SEC-3050
- FW <1.7.4 installed on CHARX SEC-3000

Fixed products.

- FW 1.7.4 installed on CHARX SEC-3150
- FW 1.7.4 installed on CHARX SEC-3100
- FW 1.7.4 installed on CHARX SEC-3050
- FW 1.7.4 installed on CHARX SEC-3000

Vulnerabilities

CVE-2025-41699

Description

An low privileged remote attacker with an account for the Web-based management can change the system configuration to perform a command injection as root, resulting in a total loss of confidentiality, availability and integrity due to improper control of generation of code ('Code Injection').

CWE: CWE-94: Improper Control of Generation of Code ('Code Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
FW <1.7.4 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
FW <1.7.4 installed on CHARX SEC-3100 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
FW <1.7.4 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
FW <1.7.4 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
FW 1.7.4 installed on CHARX SEC-3150 Order number: 1138965 (Download)
FW 1.7.4 installed on CHARX SEC-3100 Order number: 1139012 (Download)
FW 1.7.4 installed on CHARX SEC-3050 Order number: 1139018 (Download)
FW 1.7.4 installed on CHARX SEC-3000 Order number: 1139022 (Download)

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Acknowledgments

- Ryo Kato from Panasonic Holdings Corporation for reporting.

Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERTVDE for Coordination (see: https://certvde.com/en/)
- Ryo Kato from Panasonic Holdings Corporation for Reporting.

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- PCSA-2025-00015 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- VDE-2025-074: Phoenix Contact: Security Advisory for CHARX SEC-3xxx charging controllers - HTML (SELF): https://certvde.com/en/advisories/VDE-2025-074
- VDE-2025-074: Phoenix Contact: Security Advisory for CHARX SEC-3xxx charging controllers - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-074.json
- Phoenix Contact application note (EXTERNAL): https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	Tue Jul 08 12:00:00 CEST 2025	Initial Revision
1.1.0	Wed Oct 15 12:00:00 CEST 2025	Updated the reporting credits, corrected reference token for one product, fixed typo in Document notes

Sharing rules

TLP:WHITE
For the TLP version see https://www.first.org/tlp/

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany